THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number	:	09/641,929	Confirmation No: 6418
Applicants	:	Kevin G. Currans	
Filed	:	8/17/2000	
TC/A.U.	:	2131	
Examiner	:	Shin Hon Chen	
Docket Number	:	10001687-1	
Customer Number	:	022879	

Amendment after Allowance

Sir:

In response to the Notice of Allowance and Issue Fee Due mailed 5/19/05, the Applicant hereby submits new Figures 2A through 2M to replace Figures 2-1 through 2-13 as required on the Notice of Draftperson's Patent Drawing Review attached to the Notice of Allowance and Issue Fee Due. Included also are annotated sheets showing changes.

The change in the numbering of the Figures has required changes to the specification. Thus, the Applicant hereby submits pages replacement 2, 5, 6, 7, and 8 of the specification. No new matter has bee added to either the drawings or the replacement sheets.

It is not believed that additional fees are due at this time; however, if any additional fee is required in connection with the filing of this Amendment, please charge the fee to Deposit Account No. 08-2025.

Respectfully Submitted,
Kevin G. Currans

By: _____
Jeff D. Limón
Agent for the Applicants
Registration Number 45,418

Hewlett-Packard Company
Legal Department
1000 NE Circle Blvd.
Corvallis, OR 97330
Telephone: (541) 715-5979
Fax: (541) 715-8581

controlled. By way of example, if a valuable work of art such as a photograph, is digitized (i.e. converted into an electronic file), uncontrolled reproduction and distribution of the electronic file that represents the art work will eventually render the work valueless. Electronically transferring files that have any sort of economic value is problematic because of the likelihood that economic value will be taken by those who are unscrupulous.

With the advent of electronic commerce, and the accompanying worldwide distribution of documents and other valuable information, a way of discerning that a document has been delivered to, and printed by, an intended recipient might prevent or reduce instances of fraud enabled by the ease with which electronic files can be reproduced and distributed.

Summary Of The Invention

The present invention provides a method and apparatus for controlling printing of a document delivered via a computer network. A first portion of a document is encrypted using at least a first encryption key, thereby creating a partially encrypted file. The partially encrypted file is transmitted via the computer network. A second portion of the transmitted partially encrypted file is printed and a t least a serialized print number is returned. In response, the first encryption key is received. The first portion of the partially encrypted file is then decrypted and printed.

Brief Description Of The Drawings

Figure 1 is a simplified block diagram of a computer network including a sender's computer and a document recipient's computer and printer.

Figures ~~2-1 through 2-13~~ 2A through 2M show a data flow diagram or transaction timeline representation of the commands and signals exchanged between the various computers, software and printers that implement the claimed process.

Detailed Description Of The Preferred Embodiments

Briefly stated, the present invention provides a method and apparatus for verifying that a document was printed from an electronic file that was transmitted to and printed from a remote print mechanism. The exemplary method disclosed herein enables a document or file distributor to control re-distribution by conclusively determining whether a document printed

In the preferred embodiment of this invention, the recipient's computer 108 and the printer 116 are equipped with, and capable of using, the method and apparatus disclosed in "Serialized Print." As such, the printer 116 is a printer that is capable of generating serialized output as described in "Serialized Print". The disclosure and teachings of the "Serialized Print," by which the generation of serialized output is taught, is incorporated herein by reference. Using that novel method for generating serialized printed output, the printer 116 generates a unique serial number, bar code or encoded data (hereafter, serial number) for the document 114 in the course of printing the file 112. The serial number generated by the printer 116 is of paramount importance in verifying to a document sender that the file 112 was received at the computer 108 and at least partially printed.

Figures ~~2-1 through 2-13~~ 2A through 2M shows a data flow diagram depicting the steps of the method described herein.

In Figure [2-1] 2A, as an initial matter, the software capability to guarantee output print quality and to produce a serialized original print needs to be installed on the recipient's computer 108 as well as on the sender's computer 110 as depicted in step no. 202. Assuming that such software capabilities have been installed on the respective first and second computers, the recipient's (i.e. second) computer 108 will request from the printer 116 an encryption key for public distribution (i.e. a public encryption key) in the format of an X.509 certificate, which might be embodied as a serial number, a model number or combination thereof obtained from the printer in step no. 204 in Figure [2-1] 2A.

In Figure [2-2] 2B, when the printer returns an X.509 certificate and data as that identifies the capabilities of the printer (For example, is the printer capable of practicing the "Guaranteed Print " technology) at step 206, the user's computer installs the public key on a browser plug-in file, known to those skilled in the art.

Information about the X.509 standard is available from a variety of sources, including the National Institute of Standards and Technology web site, the URL of which is: http://csrc.ncsl.nist.gov/. An X.509 certificate serves as an electronic credential over the Internet for individuals and computer services (Web sites). X.509 certificates are used in the same way as birth certificates, passports or drivers' licenses to validate the identity of individuals for Web site access, communication and electronic commerce.

An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. The most widely used standard for digital certificates is X.509 which is the technology used by this merchant.

The X.509 is currently believed to be the most widely used standard for defining digital certificates. The X.509 standard for digital certificates binds the identity of a person or organization to an electronic identification key. The digital certificate contains information about its owner, its issuer, issue and expiration date stamps, and information for verifying the integrity of the certificate that can be used for digital IDs, digital signatures and electronic fingerprints.

By executing an HTTP (hypertext transfer protocol) "GET" command, the user's web browser (e.g. Internet Explorer™ or Netscape™) running on the user's computer (i.e. the second computer) requests verification of the printer's public key from a security key issuer, which then posts the answer of authenticity of the printer's public key using a "PUT" in step 207. In Figure [2-3] 2C, in step 208, a "certificate" from a printer capable of practicing the "Guaranteed Print" technology is decrypted and the printer's public key is installed (or copied) into the document purchaser's web browser. A decision to buy a document is formatted and sent to the vendor 210 conveying the capabilities of the printer, i.e. that the printer is "Guaranteed Print" technology capable.

In Figure [2-4] 2D, the document vendor's computer's response 212 is to transmit a file (identified in Figure 1 by reference numeral 112) at least part of which is encrypted at least once using a so called public key of the vendor's computer (identified in Figure 1 by reference numeral 110) and preferably also encrypted using a uniform resource locator (URL) address to which credit or payment information is to be sent by the buyer.

In an alternate embodiment, only part of a document is encrypted prior to transmission and using only one key. By encrypting only part of a document (i.e. up to a predetermined point) prior to transmission, at least the unencrypted portion of the document can be printed at the destination, without a decryption key, thereby establishing recognition-of-value by the purchaser before transferring funds. In such an embodiment, a decryption key eventually needs to be provided. By holding back the decryption key pending receipt of payment – and perhaps ascertaining proof that at least part of the document was satisfactorily printed using for example the "Guaranteed Print" teachings - a document vendor can protect its interest in the document by withholding the key until payment has been received by an entity associated with the document, for example, the vendor or a credit agency for the vender.

In step 214, the document buyer's computer (i.e. the second computer 108) optionally retrieves the URL of a credit agency and performs a secure hypertext transfer protocol transfer providing payment information to a financial organization or other credit provider effectuating the transfer of funds for the payment of the file from the vendor. A credit approval transfer form 216 is optionally returned to the buyer and enables the buyer to populate the form with pertinent credit information by which the credit provider can make payment to the vendor in step 218, shown in Figure [2-5] 2E. If the credit transaction is validated by the credit provider as set forth in step 220, the transaction can be memorialized by the buyer's computer and thereafter forwarded to the vendor in step 222, shown in Figure [2-6] 2F.

The document vendor can electronically verify with a credit provider, e.g. www.cybercash.com, in step 224 that the document purchaser has funded, or can otherwise pay for the transaction and, in response thereto, the credit provider can provide an appropriate acknowledgement 226 to the vendor, as shown in Figure [2-7] 2G. Upon verification that payment will be received by the document vendor, the vendor optionally encrypts the information content of interest, using the document vendor's private key and a second key (also known as a session key) and sends the doubly encrypted file to the purchaser in step 228. (Public key/ private key encryption and decryption mechanisms are well known. Disclosure or understanding of that technology is not germane to the invention disclosed herein. Alternate embodiments of the invention include singly encrypting the file using a single encryption key, which as an example could be the document vendor's private key, a purchaser's public key or

some other encryption key by which the document could be secured against theft in transit across a data network or by the document recipient.)

In Figure [2-8] 2H, using his own private decryption key, the purchaser decrypts the file and verifies that the received file is intact and sends the file to the printer 116 for printing in step 230. The printer begins printing the file and in the process generates an original serialized print number in accordance with the "Serialized Print" methodology, in step 232. The serial number generated by the printer will be printed and also sent to the browser of the purchaser's computer in step 234, shown in Figure [2-9] 2I. The browser also records the serial number of the print job in progress for subsequent use.

As the printer 116 continues following the instructions from the computer 108 to generate output, eventually the printer 116 or the computer 108 encounters information in the file 112 that is encrypted with the vendor's second key. Upon determining that further printing will be inhibited absent the other decryption key, the printer, using the "Serialized Print" methodology, requests the second key in step 236 from the user's computer, Figure [2-9] 2I. In step 238, Figure [2-10] 2J the user's browser transmits a request for the second key to the printer or in this case the vendor's computer 110 and as proof that the job has been at least partially printed includes the serialized print number generated by the printer in step 232.

Upon receipt of the original serial print number generated in step 232 by the vendor's computer 110 in step 238, the vendor can assume that at least part of the document file 112 was printed from the printer 116 and was fully and successfully received by the computer 108. The vendor can record the serialized print number in a database for billing purposes or for billing credit purposes.

The vendor can also optionally submit the transaction complete signal in step 240, Figure [211] 2K, to the credit provider as a means for justifying the receipt of payment from the credit provider. Upon receipt that at least part of the document has been printed, the credit provider can debit the purchasers account and credit the vendor's account accordingly.

In order to complete the printing job, the vendor's computer 110 needs to return to the purchaser's computer 108, the second decryption key in step 242 or a session key, that the printer can use for decrypting the content. The second key is encrypted so only the printer can decrypt it. This is generally done using the printer's public key and the vendor's private key. Upon receipt of the second key, the browser running on the purchaser's computer 108 passes